(12) UK Patent Application (19) GB (11) 2 348 585 (13) A

(43) Date of A Publication 04.10.2000

(21) Application No 0000704.7

(22) Date of Filing 14.01.2000

(30) Priority Data
(31) 09237226 (32) 26.01.1999 (33) US

(71) Applicant(s)
International Business Machines Corporation
(Incorporated in USA - New York)
Armonk, New York 10504, United States of America

(72) Inventor(s)
David H Jameson
Charles Philippe Louis Tresser
Chai W Wu
Steven R Abrams
Shmuel Winograd

(51) INT CL^7
G11B 20/00 , H04L 9/32

(52) UK CL (Edition R)
H4P PDCSA

(56) Documents Cited
EP 0908881 A2 EP 0901276 A2 JP 090128890 A
US 5930367 A

(58) Field of Search
UK CL (Edition R) H4P PDCSA PEP
INT CL^7 G06F 1/00 , G11B 20/00 , H04L 9/32 , H04N 1/32
ONLINE : EPODOC, WPI, JAPIO

(74) Agent and/or Address for Service
D P Litherland
IBM United Kingdom Limited, Intellectual Property Department, Mail Point 110, Hursley Park,
WINCHESTER, Hampshire, SO21 2JN,
United Kingdom

(54) Abstract Title
Method and apparatus for watermarking digital data

(57) A watermark in the form of an added message is attached to a digital recording so that a significant content of the recording is completely unchanged by the process in the sense that any reader commonly used for such recording will extract from the recording exactly what would have been extracted in the case the added message had not been attached. This is done by hiding the added message in the error correcting code (ECC) for the significant content of the recording.

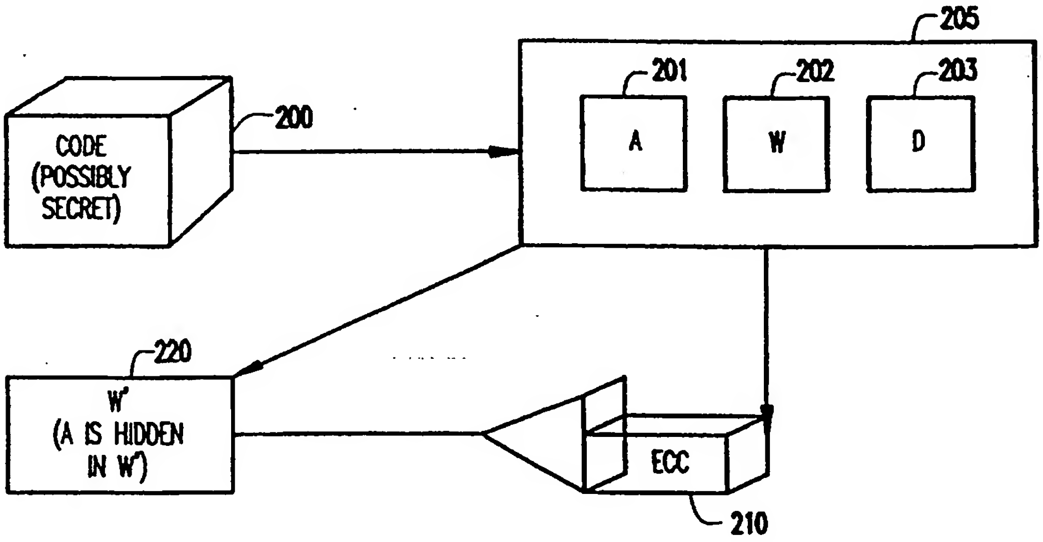

FIG.2

GB 2 348 585 A

BEST AVAILABLE COPY

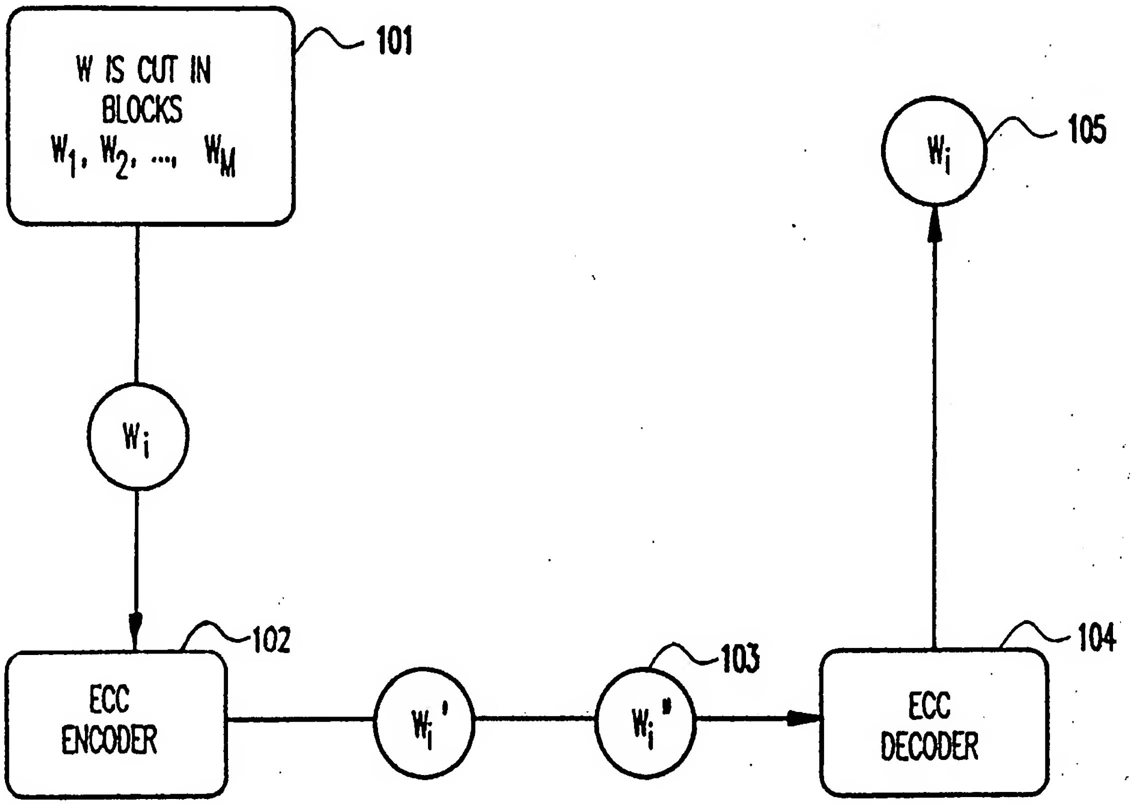
W IS CUT IN BLOCKS $W_1, W_2, \ldots, W_M$
101
W_i
102
ECC ENCODER
W_i'
W_i''
103
ECC DECODER
104
W_i
105

FIG.1

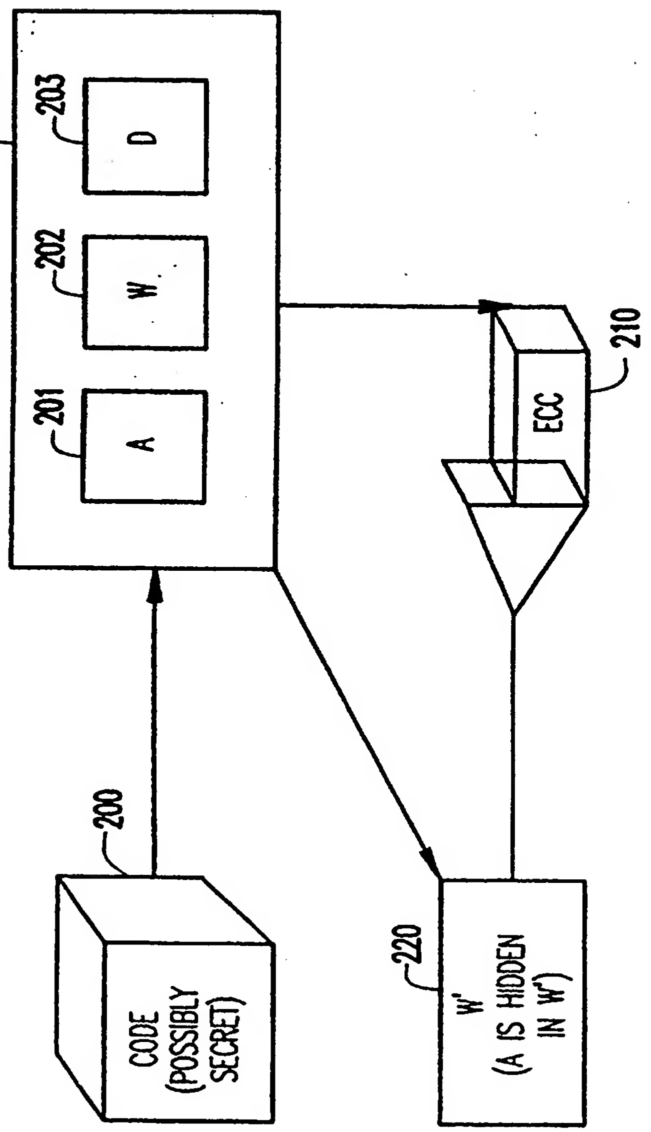
205
203
D
202
W
201
A
210
ECC
200
CODE
(POSSIBLY
SECRET)
220
W'
(A IS HIDDEN
IN W')

FIG.2

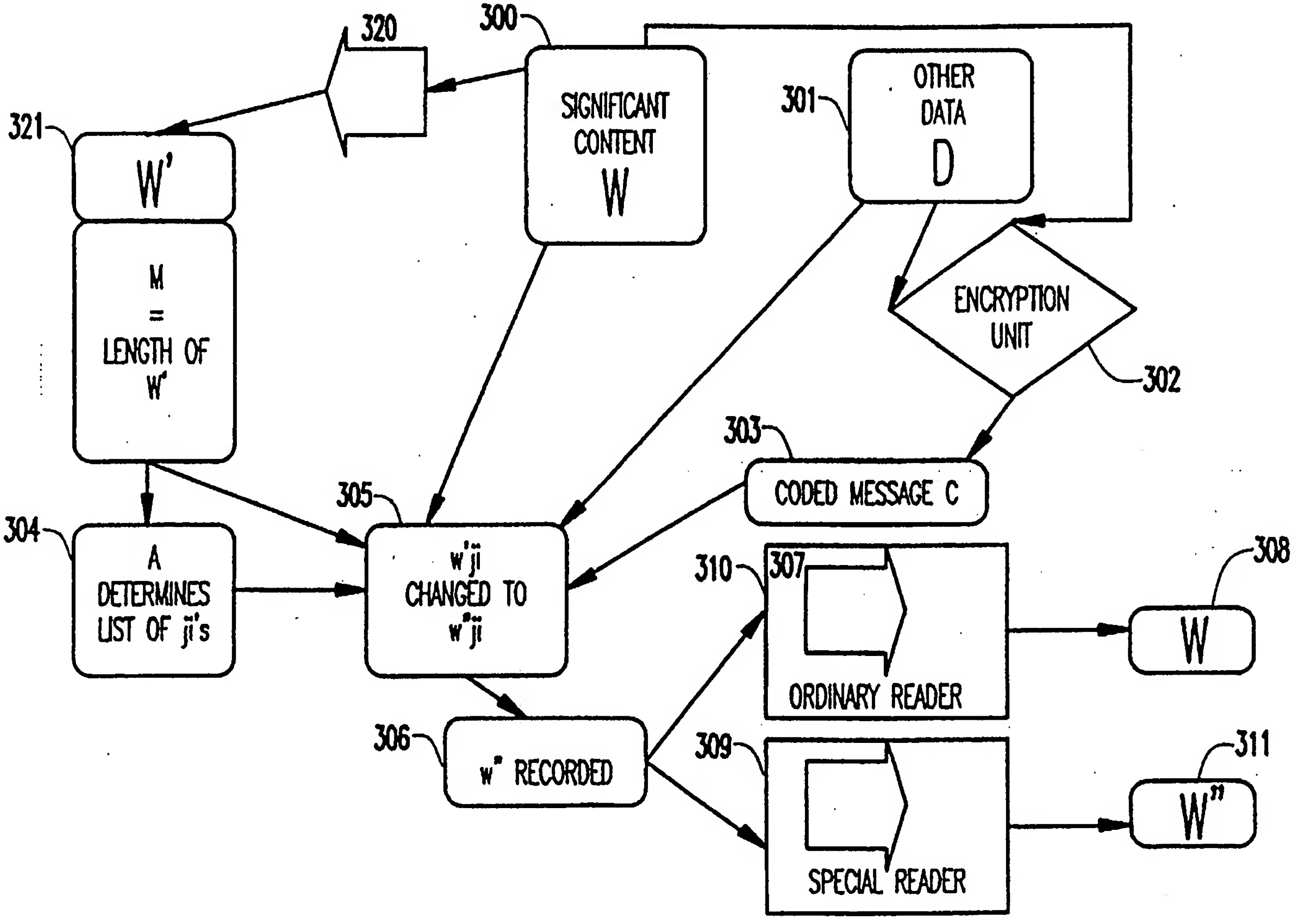
300
SIGNIFICANT CONTENT W
320
321
W'
M = LENGTH OF W'
301
OTHER DATA D
ENCRYPTION UNIT
302
303
CODED MESSAGE C
304
A DETERMINES LIST OF ji's
305
w'ji CHANGED TO w"ji
306
w" RECORDED
310
307
ORDINARY READER
309
SPECIAL READER
308
W
311
W"

FIG.3

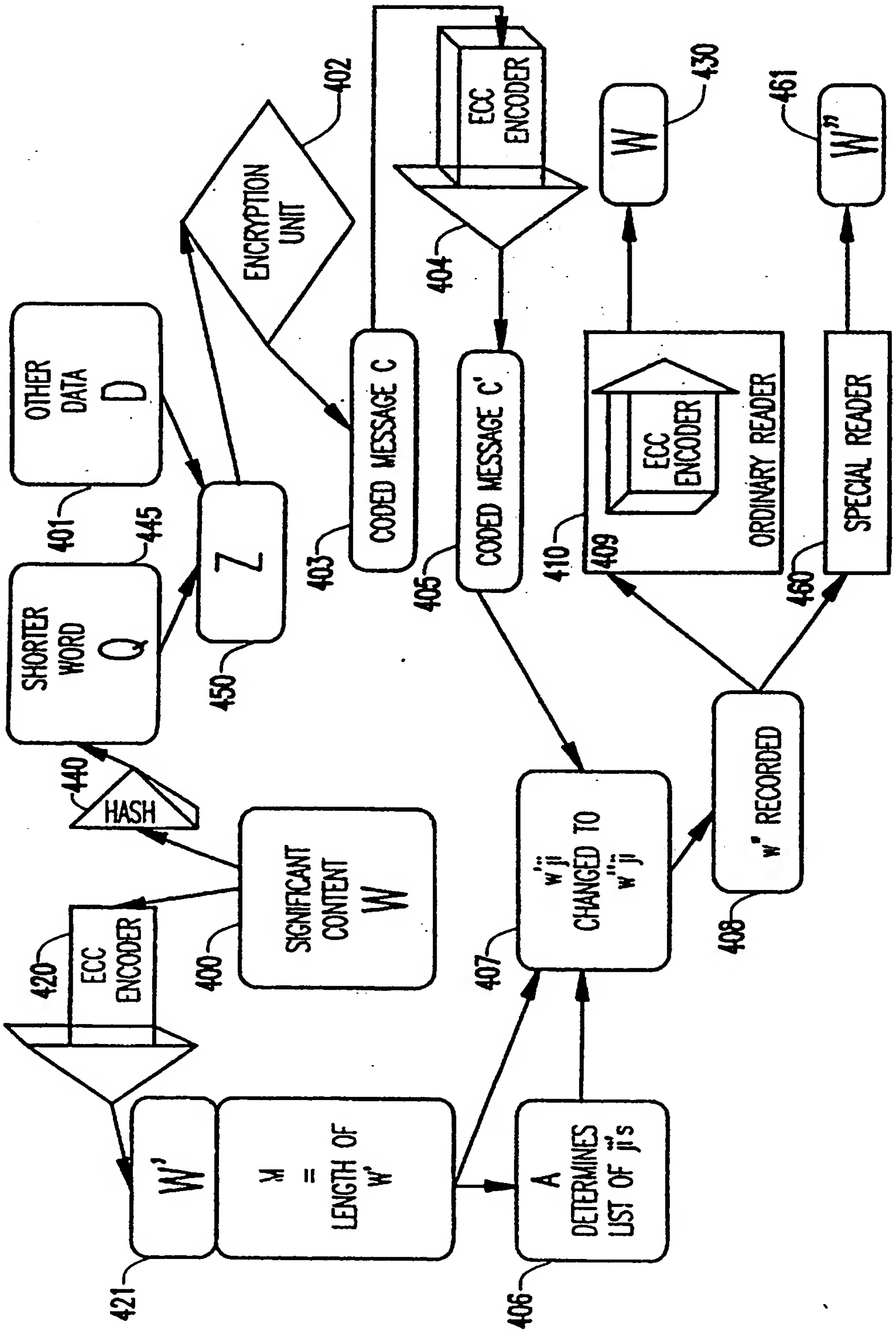
SIGNIFICANT CONTENT W
400
ECC ENCODER
420
W'
421
M = LENGTH OF W'
HASH
440
SHORTER WORD Q
445
OTHER DATA D
401
Z
450
ENCRYPTION UNIT
402
CODED MESSAGE C
403
ECC ENCODER
404
CODED MESSAGE C'
405
A DETERMINES LIST OF ji's
406
w'ji CHANGED TO w''ji
407
w'' RECORDED
408
ECC ENCODER
409
ORDINARY READER
410
W
430
SPECIAL READER
460
W''
461

FIG.4

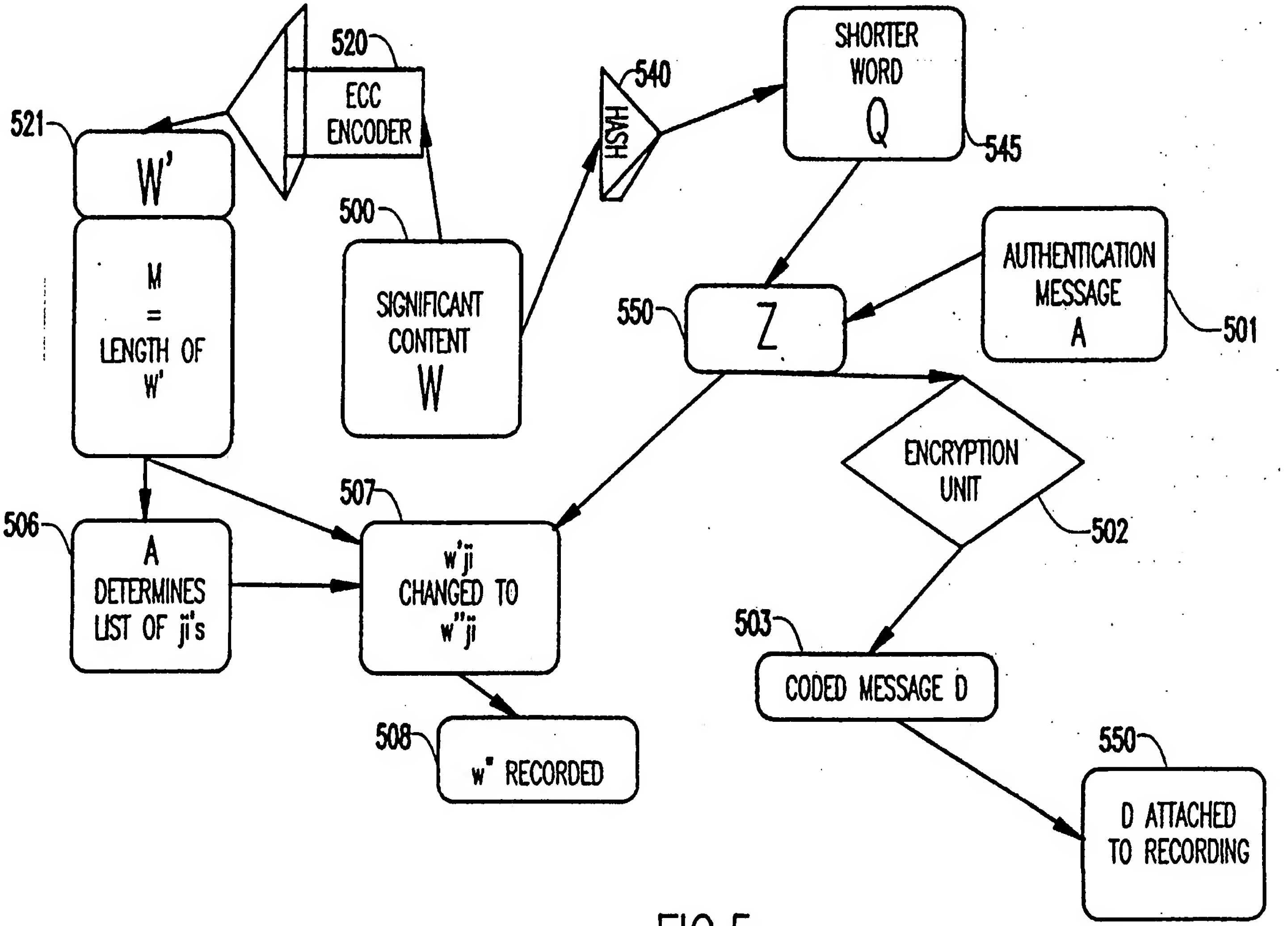
520
ECC ENCODER
540
HASH
SHORTER WORD Q
545
521
W'
500
M = LENGTH OF W'
SIGNIFICANT CONTENT W
AUTHENTICATION MESSAGE A
501
550
Z
ENCRYPTION UNIT
502
506
A DETERMINES LIST OF ji's
507
w'ji CHANGED TO w"ji
503
CODED MESSAGE D
508
w" RECORDED
550
D ATTACHED TO RECORDING

FIG.5

METHOD AND APPARATUS FOR WATERMARKING DIGITAL DATA

The present invention generally relates to a method and apparatus for preventing counterfeiting of digitally encoded media such as audio/visual and computer software compact disks (CDS) and, more particularly, to a watermarking technique for digital data.

Counterfeiting costs billions of dollars yearly to compact disk companies, software companies and other industries around the world. Several methods have been proposed to fight against counterfeiting. In US patent application Serial No.09/060,026, a coded message is associated with the combination of the significant content of the disk and a serial number on the disk. This coded message is hidden using some least significant bits of the recording. However, musicians usually consider the standard 16-bit technology used to digitize musical signals for compact disk recording insufficient to fully render the analog music quality. As a consequence, sacrificing a few bits, or even some of the least significant bits, is considered unacceptable by music producers. It is possible to intertwine the musical signal with a coded signal not made audible by the compact disk player but, in most obvious implementations at least, this would require the use of special disk readers, a solution which is clearly unappealing from a commercial point of view. It is also possible to choose the bits carrying the authentication code according to some model for musical perception in order to minimize the audible effects of changing the audio data, but this cannot be expected to be as good as keeping the full sixteen bits. It will be appreciated that in addition to music data files, other types of data files such as a computer program code would better be recorded without any change of the significant content.

The main problem solved by the present invention stems from the fact that prior methods of digital watermarking cannot be used for several types of applications, since they modify the original data set.

According to one aspect of the present invention there is provided a method for attaching an added message to a digital message so that the significant content of the digital message is completely unchanged comprising the step of hiding the added message in an error correcting code for the significant content of the digital message.

Other aspects are defined in the appended claims.

According to the invention, the basic principle is to hide all of the authentication data in the error correcting code (ECC) of the digital recording. The method of the invention can be used both to guarantee originality and to recognize counterfeiting. In the latter case, a serial number may be attached to any recording and serves, together with the significant content of the recording, to create the protecting code. A counterfeiter can only produce legitimate pairings between the serial number and the encoding by copying originals and can only duplicate as many unique, verifiable such pairs as he has access to. Depending on the size of the watermark, the probability of error in the recovered watermark due to read/write errors can be reduced by means of a second level of error correction coding.

The present invention has a significant advantage that it is not obvious that any encoding has been used (which is possibly desirable in some contexts) and that neither a special reader nor special software is necessary at the reading end, except to extract the watermark. Thus, besides music, another important application of the present invention is provided by data such as computer program code where the data is often needed with full precision and, if the format is fixed, there is no obvious space usable to embed a protecting code to guarantee that the data have not been modified.

Embodiments of the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is a flow diagram describing the general principle of error correcting codes (ECC) utilization in recording;

Figure 2 is a flow diagram representing the general mechanism of the present invention;

Figure 3 is a flow diagram representing a first preferred embodiment of the present invention;

Figure 4 is a flow diagram representing a second preferred embodiment of the present invention; and

Figure 5 is a flow diagram representing a third preferred embodiment of the present invention.

By way of background on error correcting codes, consider some significant content such as a musical recording, a musical score, a set of data, a software code, etc. Such significant content can be recorded on an optical, magnetic or other suitable media after being digitized. After the digitization the significant content takes the form of a binary word (in short, word) $W=b_1b_2...b_N$, where b_i, $i=1,2,...N$, is either 0 or 1. This word will still be considered as significant content and, in fact, when we refer to the "significant content" in the sequel, we usually mean a word such as W rather than the original image, music, data set, etc. it represents. In order to record the significant content on some chosen medium, one will usually not simply record the string of b_is as they appear in W. This is because the recording, the manipulation of the medium, the reading from the medium, and possibly some other factor, all can introduce errors which would, sometimes severely, alter the integrity of the significant content: for instance the music one would play according to the erroneously read W would be different, often quite different, from the music represented by W. Instead of recording the word W, one uses what are called error correcting codes (ECC), which have precisely the virtue of allowing some errors in strings of symbols to occur while still permitting the recovery of the word W, and thereby retrieving the significant content.

Abstractly, an ECC can be thought of as given by a many-to-one map F on the set of finite words. The inverse set $F^{-1}(W)$ of any word W to be coded contains a special subset $P(F^{-1}(W))$ which has the property that a small enough number of errors (such as bit changes and/or bit omissions and/or spurious extra bit) transform any word in $P(F^{-1}(W))$ into a word of $F^{-1}(W)$. Therefore, if one records a member of the set $P(F^{-1}(W))$ one can still recover the word W, even in the face of these sorts of errors. "Error Control Coding: Fundamentals and Applications", S. Lin and D.J. Costello, Prentice-Hall, 1983, is a general reference for the subject of error correcting codes. In practice, the ECC can be defined at the level of subwords of limited length, and for definiteness, we will limit ourselves to such ECCs, although the invention could as well be used for the more general case.

With reference to Figure 1, there is shown a flow chart of ECC with the amount of generality needed in the rest of this description. In function block 101, the word W is cut into blocks $w_1, w_2, \ldots, w_N$, where each block is made of some (usually fixed) number of successive b_is (i.e., in general, N is smaller than N). The ECC *encoder* 102 associates to each w_1 some other string of 0s and is denoted by w'_i. Each w'_i is called a *codeword*. The ordered concatenation $w'_1w'_2 \ldots w'_N$ of the w'_is form the ECC data W'. During transmission or storage, some errors might be introduced into w'_i so that, instead of w'_i, a *corrupted codeword* w''_i (block 103) is recorded. While the primary application of the invention is to get data onto a disk, the data can also be transmitted, and the same techniques can be applied to digitally encoding data on a transmission medium. That is to say that such transmission medium typically has some significant content w, which is encoded in a particular format through the use of specific error correcting codes (i.e., these are dictated by communications protocols), yielding w', which is then encoded in a specific optical, acoustic, or electrical manner for transmission on a specific medium (such as a computer local area network such as ethernet or token ring, or through a modem for transmission on a phone line, or through a digital telecommunications medium such as ISDN, or via any wireless transmission). The present invention can be used to transmit w'' instead of w'. W'' again has the property that it can be read back through an ECC decoder to yield the original word w, but can also be verified for authenticity through the use of a special reader. If the number of errors is less than a specific number (which depends on the type of ECC used), then the ECC *error correction unit* corrects the errors and returns the uncorrupted codewords w'_i. When w'_i is decoded in the ECC *decoder* 104, the word w_i (output 105) is given as the output of decoder 104.

In general, the average length of w'_i is bigger than that of w_i. What really matters is that not only w'_i, but also any string of 0s and 1s obtained from w'_i by making at most K errors (where K and the type of allowed errors depends on the chosen ECC (and possibly on w_i)) is corrected by 104 and decoded by decoder 104 to generate w_i. In the sequel, we will always assume that $K>2$, which can be easily achieved by any of the currently used ECC, such as the Reed-Solomon code.

With reference first to Figure 2, some authentication data A 201 is associated to any data set W 202 to be recorded. The basic principle used is to hide all of the authentication data in the error correcting code 210 used to perform the recording. Following the teaching of US application Serial No. 09/060,026, the authentication data A may be chosen to be such that the triple (A,W,D) at 205, formed by the authentication data A, the data set W, and some other auxiliary data set D 203 (associated to W or to the physical support of the recording) cannot be generated by unauthorized parties. The code used for the generation of such triples can be based on (secret or public) encryption 200. In particular, instead of the general implicit relation between A, W and D, the authentication message A may be a coded message depending on the pair (W,D), in which case we will often write C instead of the generic notation A. Depending on the precise implementation, the present invention allows recognizing the originality and/or legitimacy of recordings in such a way that the meaning of what is recorded is completely unaffected by the implementation of the invention and standard readers would neither detect nor be affected by the implementation of the invention.

We note that using some of the error correcting codes to carry authentication data may, in general, reduce the robustness of the error correction scheme. That is, while the original system may have been able to correct K errors, a system using our invention may now be able to correct K'<K errors. This is not viewed as a significant problem, as common delivery media such as the compact disk (CD) are capable of correcting far larger numbers of errors than are generally required (see, for example, "Phillips-Sony Red Book" or International Electrotechnical Commission standard IEC 60908 (1987-09), for detailed information on the Compact Disc standard). It will be understood by those skilled in the art that the CD standard provides certain *subcode* channels, i.e., channels which contain non-audio data. Any of these might trivially be used to carry digital signatures or watermarks. However, the invention still has utility for storage medium other than the standard CD, or for audio CDs in which the subcode channels are otherwise in use, as well as in the transmission medium which have no unused subcode channels. In fact, in any particular embodiment, it should be possible to carefully distribute the authentication data across the medium so as to distribute the reduction in robustness as appropriate. For example, the robustness of the error correction scheme can be compromised in less critical areas of the data set or better-protected areas of the physical medium, or evenly distributed across the data set to minimize the aggregate impact. Furthermore, in certain medium, again such as CDs, in addition to the use of error correction codes, the data is interleaved on the physical medium in a manner which makes the data recovery process exceptionally robust in the face of specific types of errors; e.g., burst-errors, and errors located in physically contiguous regions of the medium. Appropriate distribution of the additional authentication data can help preserve these sorts of robust behaviors.

A description of the specific cryptographic techniques used herein (secret key/public key (SK/PK) pairs and hash functions) can be found in *Handbook of Applied Cryptography* by Alfred J. Menezes, Paul C. van Oorschotand and Scott A. Vanstone, CRC Press, 1997.

A first embodiment of the invention will now be described with reference to Figure 3. The significant content $W=w_1w_2...w_N$ at input block 300, possibly combined with supplementary data D at input block 301 (such as time, data and/or serial numbers attached physically to the recording), is encrypted by a secret key S1 in the encryption unit 302 to generate a coded message C at 303. The coded message C can be represented as some sequence $s_1s_2...s_c$ of 0s and 1s. For convenience, we will assume that the length c of C is fixed once and for all, but this is quite inessential to the invention and other conventions can be taken as well. At the FCC encoder 320, the word W is transformed to the primary error corrected word $W'=w'_1w'_2...w'_M$ of length M at 321 (in general, M is greater than N). A defined algorithm A at 304 associates to M a collection j1<j2<. ..<jc<M of addresses of coding blocks $w'_{j1}, w'_{j2}, \ldots, w'_{jc}$. For instance, one can take the w'_{ji}s, with *i* in {1,2,...c}, as evenly distributed along W'. The choice of (j1,j2...,jc) can be either secret or known publicly. These selected coding blocks are changed in *305* into w''_i according to another (possibly secret) key S2, i.e., w'_{ji} is changed into $w''_{ji}=S2(w'_{ji},W.D.C)$. We denote by W' the ECC transform of W, and by W" the word obtained from W' by replacing each coding block w'_{ji} by w''_{ji}.

The word W" is what gets recorded at function block 306. When read with an ordinary reader 310, W" goes through an ECC decoder 307 to yield back W if there has not been too many errors.

To check that the recording is original, one needs a special reader at 309 which accesses W" and delivers it without passing through the FCC decoder 307. The mechanism for reading W" is part of commercially available audio-CD and CD-ROM players, and will be understood by those skilled in the art. A special reader can be constructed by intercepting the signal before it reaches the error correcting circuitry.

One can then verify that C is as it should be given significant content W and other data D. More precisely because of errors, the C one reads with the special reader 309 may be slightly different from the original C. To verify authenticity of the encoding, one verifies that the rate of errors in the coding blocks is of the same order as in the rest of the recording.

Because of the errors which may occur in the coding blocks, public key encryption cannot be readily adapted to the embodiment represented in Figure 3. Two embodiments will therefore be described which allow the use of public key encryption as this is often the most convenient method to ensure secure and easy verifiability as then several agents can verify authentication codes, but far less can generate them.

A second embodiment will next be described with reference to Figure 4. The significant content $W=w_1w_2\ldots w_N$ at input block 400 goes through a secure, publicly known, hash function at function block 440 to yield a much shorter word Q at output 445. The word Q is then possibly concatenated with supplementary data $D=x_1x_2\ldots xd$ at input block 401 (such as time, data and/or serial numbers attached physically to the recording) to form a word $Z=u_1u_2\ldots u_p$ at output 450 (if there is no D, Z is just Q). The word is encrypted by a secret key S1 in the encryption unit 402, the secret key being now chosen as the secret part of a secret key/public key (SK/PK) pair, to generate a coded message C of length c at output 403. The coded message C can be represented as some sequence $s_1s_2...s_c$ of 0s and 1s.

At the ECC encoder 420, the word W is transformed to the word $W'=w'_1w'_2...w'_M$ of length M at output 421 (in general, M is greater than N). Next a second ECC encoder at 404, converts C into ECC code words $C'=t_1t_2...t_{c'}$ of length c'>c at output 405. Note that the second error correcting code used at ECC encoder 404 does not have to be the same as the ones used at ECC encoder 420. To distinguish this ECC encoder/decoder pair from the first FCC encoder/decoder pair, we will call this the *secondary ECC encoder/decoder*.

A defined algorithm A at function block 406 associates to M a collection j1<j2<...<jc'<M of addresses of *coding blocks* $w'_{j1}w'_{j2},...w'_{jc}$. For instance, one can take the w'_{ji}s, with *i* in {1,2,...c}, as evenly distributed along W'. The choice of (j1,j2,...,jc') should be known publicly, or at least by whomever one wants to be able to check the authenticity of the recording. These selected coding blocks are changed in function block 407 into $w''_{ji}=f(t_i,w_{ji})$ in such a way that w"can be interpreted as a 0 or a 1 according to a publicly known rule. Also, the function f is such that there is a map g satisfying $t_i=g(w''_{ji})$. We denote by W' the ECC transform of W, and by W" the word obtained from W' by replacing each coding block w'_{ji} by w''_{ji}. The word W" is such that any reading of the word $w''_{j1}w''j2...w''_{jc}$ which is not to much spoiled by errors is interpreted as C by running the secondary ECC decoder on the word

$$g(w''_{j1})g(w''_{j2})...g(w_{jc}')$$

The word W" is what gets recorded at 408. When read with an ordinary reader 410, W" goes through an ECC decoder at 409 to yield back W at output 430 if there has not been too many errors.

To check that the recording is original, one needs a special reader (as described previously) at 460 which accesses W" and delivers it without passing through the ECC decoder.

One can then verify that C is as it should be given W and D, using the public part of the SK/PK pair. This check of authenticity may be performed by a specialized reader which also outputs the significant content W, so that authentication can be performed while inspecting W. In case this invention is used to protect retail items, the manufacturer may require the retailers selling its brand to use only such an authenticating reader when customers want to inspect W.

A third embodiment will now be described with reference now to Figure 5. The significant content $W=w_1w_2..\ .w_N$ at input block 500 goes through a secure, publicly known, hash function at function block *540* to yield a much shorter word Q at 545. The word Q is then concatenated with an authentication message $A=u_1u_2...u_a$ at input block 501 to form a word $Z=t_1t_2...t_p$ at output 550. The word Z is encrypted by the secret part S1 of a SK/PK pair in the encryption unit 502 to generate a coded message D at output 503.

At the ECC encoder 520, the word W is transformed to the word $W'=w'_1\ w'_2...w'_M$ of length M at 521 (in general, M is greater than N). A defined algorithm **A** at function block 506 associates to M a collection j1<j2<...<jc'<M of addresses of *coding blocks* $w'_{j1},w'_{j2},...,w'_{jc}$. For instance, one can take the w'_{ji}s, with *i* in (1,2,...c}, as evenly distributed along W'. The choice of (j1,j2,...,jc') should be known publicly, or at least by whomever one wants to be able to check the authenticity of the recording. These selected coding blocks are changed in function block 507 into $w''_{ji}=f(u_i,w_{ji})$ in such a way that w" can be interpreted as a 0 or a 1 according to a publicly known rule. Also, the function f is such that there is a map g satisfying $u_i=g(w''_{ji})$. Again the choice of f and g should be known publicly, or at least by whomever one wants to be able to check the authenticity of the recording. We denote by W" the FCC transform of W, and by W" at 508 the word obtained from W' by replacing each coding block w'_{ji} by w''_{ji}. A specialized reader can extract the word Z from the recording.

Because of errors, what is actually read (assuming the recording is authentic) will be a approximation Z' to Z, this approximation being close if there are not yet too many errors. The word D is also attached to the recording at 550 (for instance in the form of a bar code on the physical support of the recording) and one checks authenticity by verifying that Z' is close enough to the word Z extracted from D by the public part of the SK/PK pair.

Thus has been described a method and apparatus which permits recognition whether a recording is original and/or if it has been performed by the legitimate originator. Furthermore, the method and apparatus provide a way to authenticate a digital recording where no significant bit of the recording can be modified for purposes of the authentication. Still further, the described watermarking technique protects the recordings from counterfeiting while avoiding the need for special apparatus for reading the recordings.

While the invention has been described in terms of three preferred embodiments, those skilled in the art will recognize that the invention can be practiced with modification within the scope of the appended claims.

CLAIMS

1. A method for attaching an added message to a digital message so that the significant content of the digital message is completely unchanged comprising the step of hiding the added message in an error correcting code for the significant content of the digital message.

2. The method of claim 1, further comprising the step of encrypting at least a portion of the significant content to generate the added message.

3. The method of claim 2, wherein the step of encrypting uses a public key encryption method.

4. The method of any preceding claim, wherein two or more layers of error correction are used in the error correcting code.

5. The method of any preceding claim, wherein a second data set is attached to the digital message.

6. The method of claim 5, wherein the second data set is attached to a physical support of the digital message.

7. The method of claim 6 further comprising the step of reading said added message to check that the physical support of the digital message has not been counterfeited.

8. The method of claim 1, further comprising the step of reading said added message to check that the significant content of the digital message is authentic.

9. The method of any preceding claim wherein the digital message is stored in a recording.

10. The method of claim 9 further comprising the steps of:

decoding the error correction code; and

reading the added message to check that the physical support of the recording has not been counterfeited.

11. The method of claim 9 further comprising the steps of:

decoding the error correction code; and

reading said added message to check that the significant content of the recording is authentic.

12. The method of claim 1 further comprising the step of transmitting the added message and the significant content.

13. The method of claim 1 wherein the digital message is transmitted over a transmission medium, and said added message is hidden in the error correcting code specific to said transmission medium.

14. A method for attaching an added message to a digital recording so that a significant content of the digital recording is completely unchanged, comprising the steps of:

selecting an added message that is to be attached to the significant content;

associating the added message with the significant content;

selecting an error correction code for the significant content; and

hiding the added message within the error correction code.

15. The method of claim 14 wherein the digital message is stored in a recording.

16. The method of claim 14 wherein the digital message is transmitted over a transmission medium.

17. Digital recording apparatus including:

means for recording a significant content onto a recording medium;

means for associating an added message with said significant content;

a means for selecting an error correction code for the significant content; and

a means for hiding the added message within said error correction code.

18. Data processing apparatus comprising:

means for generating a digital message with a significant content;

means for associating an added message with said significant content;

means for selecting an error correction code for the significant content;

means for hiding the added message within said error correction code; and

means for transmitting the added message and the significant content.

19. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for attaching an added message to a digital recording so that a significant content of the digital recording is completely unchanged, said method step comprising hiding the added message in an error correcting code for the significant content of the digital recording.

20. A program storage device readable by a machine, tangibly embodying a program of instructions executable by the machine to perform method steps for attaching an added message to a digital recording so that a significant content of the digital recording is completely unchanged, said method steps comprising:

associating an added message with the significant content;

selecting an error correction code for the significant content; and

hiding the added message in an error correcting code for the significant content of the recording.

CHARTER MARK

The Patent Office

INVESTOR IN PEOPLE

13

Application No:	GB 0000704.7	**Examiner:**	Ken Long
Claims searched:	1 to 20	**Date of search:**	21 July 2000

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.R): H4P (PDCSA & PEP)

Int Cl (Ed.7): H04L 9/32, G11B 20/00, H04N 1/32 & G06F 1/00.

Other: ONLINE : EPODOC, WPI, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage		Relevant to claims
X P	EP 0908881 A2	TOSHIBA (page 2 lines 34-54)	1, 14, 17 & 18 at least
X P	EP 0901276 A2	HITACHI (page 2 lines 34-54)	1, 14, 17 & 18 at least
X	US 5930367	SONY (See column 1 lines 35-55, column 2 lines 17-26 and column 4 line 47 to column 5 line 4 of the US document.)	1, 2 and 8 to 18
&	JP 09 128890	SONY (This is JP equivalent of US 5930367 and was published on 16 May 1997)	1, 2 and 8 to 18

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.